

Index

A

AcceptEnv 362, 372
ACK 88
ACL 230
AdressFamily ... 372, 421
AFS 30
Agent 134, **251**
 Sicherheit 266
 Weiterleitung 261
AH 35, 99
Alice 46
AllowGroups ... 355, 372
AllowTcpForwarding 372
AllowUsers 355, 372
ARP 94
ASCII 83
Authentifizierung **12, 17,**
 70, 113
 Agent **134**
 BSD 329
 Challenge/Response ..
 328
 hostbased 324
 keyboard-interactive ..
 195
 Methoden **126, 189, 321**
 mit Kerberos 341
 per GSSAPI 347
 per Passwort .. **128, 339**
 per RHost **129**
 per RHostRSA **133**
 per RSA1 **131**

 Protokoll **186**
 publickey 332
 Varianten 13
authorized_keys 333,
 388
 Schlüsselattribute . 336
AuthorizedKeysFile . 373
autoconf 285
Autorisierung **12, 15**

B

Banner 360, 373
BatchMode 421
Berechenbarkeit
 effiziente 57
BindAddress 421
Bob 46
border router 98
Brute-Force Angriff .. 184
Brute-Force Angriff .. 137
Brute-Force Angriff 65, 95
Bubblebabble 457
buffer overflow 159

C

CA 160, 272
Carrier 548
CBC 47, 155, 184
CERT 139
Certification Authority ..
 siehe CA
CFB 47, 140
Challenge 131

 -Response 153, 328
ChallengeResponseAu-
 thentication . 373, 422
check-file 241
CheckHostIP 422
Checksumme 57
chosen plaintext attack ..
 66, 132
chroot 296, 522
CIDR 558
Ciphers 373, 422
classful routing 559
ClearAllForwardings 422
ClientAliveCountMax ...
 373
ClientAliveInterval . 352,
 374
Compression ... 374, 423
CompressionLevel ... 423
configure 285
connection redirection ...
 142
ConnectionAttempts 423
ConnectTimeout 423
ControlMaster .. 424, 575
ControlPath 425, 575
CRC 57, 119, 272
CRLF 240
CVS 19, 521, 575

D

Datagramm 85
de Raadt, Theo 34

- Denial of Service .. 93, 97,
159, 184
DenyGroups 355, 374
DenyUsers 355, 375
Dienst 78
Diffie-Hellman .. 63, 149,
179, 455
 Group Exchange .. 156
digest 57
digitale Signatur 55
digitale Signatur **58**
DISPLAY .. 214, 215, 395,
497
DNS
 lookup 101
DNSSEC ... 149, 156, 195
Draft 111
Dropbear 25
DSS 160, 182
DynamicForward 425
- E**
ECB 47
Egress 98
EnableSSHKeysign . 326,
426
Escape-Zeichen *siehe*
 EscapeChar
EscapeChar 281, 426
ESP 35, 99
eval 573
ExitOnForwardFailure ...
427
exploit 32
- F**
Fälschungssicherheit .. 57
facility code 365
Faktorisierung 67
filename-charset 240
Filterung
 Egress- 98
 Ingress- 99
Fingerabdruck *siehe*
 fingerprint
fingerprint 57
Firewall **38**, 208
- ForceCommand 375
ForwardAgent 427
Forwarding . 29, 208, **482**
 dynamisch 398, 491
 Einschränkungen bei ..
 213
 IP 563
 lokal . 210, 318, 400, 485
 off-host 211, 494
 remote 211, 488
 X11 213, 495
ForwardX11 428
ForwardX11Trusted . 428
Frame 81
FreeNX 519
freeSSHD 25
Freie Software 21
Friedl, Markus 34
- G**
gated 560
Gateway 559
GatewayPorts ... 375, 428
Geheimhaltung 13
gemeinsames Geheimnis
 siehe shared secret
Gleichverteiltheit 57
GlobalKnownHostsFile ..
429
GnuPG 41
GSSAPI 149, 155, 182,
196, 197, 271, 347
 und Kerberos 348
GSSAPIAuthentication ..
376, 429
GSSAPICleanupCreden-
tials 376, 429
- H**
Hallo Welt 278
Hashfunktion **56**
HashKnownHosts ... 429
Header 78, 86
home-directory 241
Host 429
HostbasedAuthentication
 376, 430
- HostKey 376
HostKeyAlgorithms . 430
HostKeyAlias 430
HostName 431
hosts.equiv ... 36, 129
Hybridverfahren **53**
- I**
IDEA 23, 140
Identifikation 13
Identität 13
IdentitiesOnly 431
identity.pub 334
IdentityFile 431
IETF 111
ifconfig 565
IgnoreRhosts 377
IgnoreUserKnownHosts .
377
IMAP 20
informationelle
 Selbstbestimmung 12
Ingress 99
insertion attack 120
Integrität .. 12, **14**, 59, 71,
170, 174
 Verlust 15
Internet Service Provider
98
Intranet 38
IP 84
 Adresse 86
 Forwarding 563
IPsec 34, 550
IRC 579
ISO/OSI **80**
ISP . *siehe* Internet Service
 Provider
- K**
Kanal 205
 Typen 206
 Verwaltung 205
Kanonisierung 233
KbdInteractiveDevices ..
432
KDC 38

-
- Kerberos 30, **38**, 201, 341, 348
 - Tickets 38
 - KerberosAuthentication . 377
 - KerberosGetAFSToken .. 377
 - KerberosOrLocalPasswd 377
 - KerberosTicketCleanup .. 377
 - keyboard-interactive 153
 - KeyRegenerationInterval 378
 - known plaintext attack .. 66, 118
 - known_hosts 160
 - Hashing 469
 - Kollisionswiderstand . 56
 - Kompression 175
 - kompromittierende
 - Kanäle 69
 - Kryptoanalyse 44
 - Kryptographie 20, **43**
 - aktiver Angriff 64
 - Algorithmen **44**
 - Anforderungen . 67, 73
 - asymmetrische **51**
 - Grundaufgaben 12
 - hybride **53**
 - Kompromittierung . 71
 - Kryptoanalyse 64
 - passiver Angriff 64
 - Schlüssel **44**
 - Schlüssellänge 45
 - symmetrische **48**
 - L**
 - Lindstrom, Ben 34
 - ListenAddress .. 304, 352, 378
 - LocalCommand . 432, 565
 - LocalForward 432
 - LoginGraceTime 353, 378
 - LogLevel ... 365, 378, 432
 - loopback 213
 - lsh 25
 - M**
 - MAC 55, **57**, 158, 174, 272
 - MACs 379, 433
 - MacSSH 25
 - make 283
 - Man-in-the-middle ... 14, 17, **66**, 95, 138, 159
 - Masquerading 559
 - Match 379
 - MaxAuthTries .. 305, 353, 380
 - MaxStartups 353, 380
 - McIntyre, Jason 34
 - Message Authentication Code *siehe* MAC
 - message integrity code .. 200
 - Migration 529
 - r-Kommandos 529
 - SSHV1 nach v2 533
 - Ziel-Szenario 538
 - Miller, Damien 34
 - MindTerm 26
 - motd 359
 - Multiplexing 205
 - N**
 - Nagios 517
 - NAT 559
 - NCP 553
 - netcat 578
 - newline 240
 - NFS 89, 230
 - Nichtabstreitbarkeit .. 12, **15**, 71
 - NNTP 208
 - NoHostAuthentication-ForLocalhost 433
 - nologin 362
 - nsswitch.conf 588
 - NumberOfPassword-Prompts 433
 - NX 519
 - O**
 - OFB 47
 - Open Source 20
 - OpenBGPD 560
 - OpenBSD 573
 - OpenOSPF 560
 - OpenPGP 41, 182
 - OpenSSH 26
 - Agenten 470
 - Client 314, 394
 - Compile-Time Optionen 350
 - Identitäten 452
 - Infrastruktur 443
 - Installation 282
 - Konfiguration 290, 350, 394
 - Lizenz 28
 - Logging 365
 - Migration 529
 - portierte Version 28
 - Server 302, 350
 - Subsystem 364
 - Variablen 298
 - Verbreitung 26
 - Zugriffskontrolle .. 296
 - OpenSSL 28
 - OpenVPN 551
 - opportunistic encryption 549
 - P**
 - packet injection 141
 - Padding 118, 158
 - PAM 196, 283, 342
 - Passphrase 454, 571
 - ändern 468
 - PasswordAuthentication 380, 434
 - Perfect Forward Secrecy . 63, 71, 170
 - PermitEmptyPasswords . 305, 381
 - PermitLocalCommand .. 434
 - PermitOpen 381
 - PermitRootLogin 359, 381
 - PermitTunnel ... 382, 564
 - PermitUserEnvironment . 382, 391

- PFS *siehe* Perfect Forward Secrecy
PGP 41
phishing 101
PidFile 382
ping 565
ping of death 97
Pipe 279
PIX 552
PKI 157, 243, 272
POP 19, 208
Port 383, 434
Port-Weiterleitung .. *siehe* Forwarding
PPP 19
PPTP 552
Prüfsumme 71, 119
PreferredAuthentications 434
PrintLastLog 360, 383
PrintMotd 359, 383
Private Adreßräume . 559
PROPOSED STANDARD 145
Protocol 383, 434
Protokoll 77
 Authentifizierungs- ... 186
 Transport- 170
 Verbindungs- 204
Provos, Niels 34
Proxy 19, 215
 reverse 216
 SOCKS 19
ProxyCommand 434
PubkeyAuthentication ... 383, 435
public key 51
public key 60
 -Subsystem ... **154, 243**
 -Verfahren 181
 File Format **154**
public scrutiny 20
PuTTY 30
- Q**
Quagga 560
- Quota 242
- R**
r-Kommandos 17, 36, 69, 529
RADIUS 36, 329
Random Early Detection . *siehe* RED
RC4 140
rcsshd 306
REALPATH 233
RED 354
Red Hat Package Manager . *siehe* RPM
reexec 308
Referenzmodell 76
RekeyLimit 435
RemoteForward 436
replay attack .. 65, 94, 100
resolv.conf 588
RFC 32, 111
 .rhosts ... 129, 138, 325
RhostsRSAAuthentication 384, 436
Rice, Tim 34
root
 Privilegien 22
round-trip 171
route 565
Router
 Grenz- *siehe* border router
Routing
 classful 559
 classless inter-domain . 559
 Tabelle 560
RPM 282
RSA 29, 71, 182
RSAAuthentication . 384, 436
rsync 531, 576
- S**
SA 35
SAD 35
Schicht 77
- Abstraktion durch .. 78
Anwendungs- .. 83, 90
Bitübertragungs- ... 81
Darstellungs- 83
Sicherungs- 81
Sitzungs- 82
Transport- 82, 87
Vermittlungs- 81
- Schlüssel
 Austausch **62**
 Management 68
Schlüsselaustausch .. 175
Schnittstelle 78
scp 18, 148, 152, 389, 504
screen 571, 574
SDCTR 47, 155
SECSH 111
Secure Shell
 Ein/Ausgabeumleitung 279
secure by default 303
Secure Hash Algorithm .. *siehe* SHA-1
Secure Shell **109**
 Abwärtskompatibilität **167**
 Algorithmen 270
 Architektur 269
 Secure Shell
 Authentifizierungsver-
 fahren 271
 Client 114
 Erweiterbarkeit ... **167, 269**
 Grundsätze 112
 Integrität 272
 Kanäle 271
 Protokoll 110, **117**
 Session 115
 v1 109, **117**
 v2 109, **145**
 Zertifikate 272
SecureCRT 31
SendEnv 362, 436
ServerAliveCountMax ... 437

-
- ServerAliveInterval .. 437
 - ServerKeyBits 384
 - Session
 - hijacking 93, 94
 - killing 93, 94
 - SFTP 18, 152, **218**, **509**
 - Dateihandle 231
 - extension 229
 - Fehlercodes 234
 - Paketaufbau 220
 - Paketverarbeitung . 223
 - Protokollerweiterungen 236
 - Protokollstruktur .. 222
 - Sicherheit 241
 - URL **165**
 - SHA-1 178
 - shared secret 64
 - .shosts 325
 - Sicherheit
 - Ende-zu-Ende 105
 - Endgerät 105
 - in Schichten 104
 - Koppelement 105
 - Signatur
 - digitale 55, **58**
 - Single Sign-On . 153, 252, 572
 - Sitzung
 - Übernahme *siehe* Session hijacking
 - Abbruch . *siehe* Session killing
 - interaktive 136, 207
 - Sitzungsschlüssel ... 116, 124, 175
 - SmartcardDevice 438
 - SMTP 208
 - smurf attack 97
 - sniffing 94, 100
 - social engineering 69
 - SOCKS 210, 491, 578
 - source routing 17, 94, 102
 - space-available 241
 - SPI 35
 - SPKI 182
 - SPNEGO 200
 - spoofing 138
 - DNS 17, 94, 100
 - IP 17, 94, 96
 - SSH ... *siehe* Secure Shell
 - SSH Communications
 - Security 33
 - ssh-add 474
 - ssh-agent 472, 572
 - ssh-askpass 573
 - ssh-keygen 455
 - ssh-keyscan 479
 - SSH-URL **164**
 - SSH_ASKPASS 395
 - ssh_config ... 294, 395, 416
 - sshd_config . 293, 303, 351, 366
 - SSHFP . 156, 413, 461, 468
 - sshrpc 361
 - SSL **39**
 - Steves, Kevin 34
 - sticky bits 242
 - Stopfdaten *siehe* Padding
 - StrictHostKeyChecking .. 438
 - StrictModes 384
 - Subsystem 384
 - supported2 238
 - SYN 88
 - sysctl 563
 - SyslogFacility ... 365, 384
- T**
- tap-Interface *siehe* tun/tap-Interfaces
 - TCP 87
 - Port 88
 - Sequenznummer ... 89
 - TCP/IP **84**
 - tcpdump 568
 - TCPKeepAlive . 352, 385, 439
 - Tectia Secure Shell 31
 - three-way-handshake . 88
 - TLS **39**, 152
 - Token 83
 - traceroute 566
 - Transportprotokoll .. 170
 - Tucker, Darren 34
 - tun/tap-Interfaces ... 555
 - tunctl 563
 - Tunnel 19, 208, 439
 - TunnelDevice 440
- U**
- UDP 85, 89
 - Unicode 83
 - Unumkehrbarkeit 56
 - Urheberschaft 59, 71
 - URI 152, 163
 - UseDNS 385
 - UseLogin 385
 - UsePAM 341, 386
 - UsePrivilegedPort ... 440
 - UsePrivilegeSeparation .. 386
 - User 440
 - UserKnownHostsFile 440
 - UTF-8 83, 240
- V**
- vendor-id 237
 - Verbindlichkeit 15
 - Verbindungsparameter .. 164
 - Verbindungsprotokoll ... 204
 - Sicherheit 215
 - verdeckte Kanäle 184
 - VerifyHostKeyDNS .. 440
 - Verschlüsselung *siehe* Kryptographie
 - version-select 237
 - Vertraulichkeit 12, **13**, 17, 70, 170, 172
 - Virtual Private Network . *siehe* VPN
 - VNC 19
 - VPN 19, **547**
 - auf Schicht 2 569
 - Client-zu-Client ... 555
 - debuggen 566
 - Netz-zu-Client 554

Index

- Netz-zu-Netz 554
- W**
- web of trust 37
- Weiterleitung *siehe*
Forwarding
- Wildcards 299
- WinSCP 32
- X**
- X.509 ... 40, 149, 157, 272
- X11 213
 - magic cookie 217
- X11DisplayOffset 386
- X11Forwarding 386
- X11UseLocalhost 386
- xauth 503
- XAuthLocation . 387, 441
- Xauthority 29
- xterm 280
- Y**
- Ylönen, Tatu 33
- Yonan, James 551
- Z**
- Zebra 560
- zlib 30